Eiropas Savienības
Oficiālais Vēstnesis

LV
L sērija

2024/1942

20.12.2024.

KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2024/1942

(2024. gada 5. jūlijs),

ar ko nosaka kopīgas procedūras un sīki izstrādātus noteikumus attiecībā uz kompetento iestāžu piekļuvi kravu pārvadājumu elektroniskai informācijai un tās apstrādi saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2020/1056

(Dokuments attiecas uz EEZ)

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES) 2020/1056 (2020. gada 15. jūlijs) par kravu pārvadājumu elektronisku informāciju ([1]), jo īpaši tās 8. pantu,

tā kā:

(1) Regulā (ES) 2020/1056 ir noteikts, ka dalībvalstīm jānodrošina, lai visām to kompetentajām iestādēm būtu piekļuve kravu pārvadājumu elektroniskai informācijai (“*eFTI*”) saskaņā ar kopīgām procedūrām un sīki izstrādātiem noteikumiem, tai skaitā kopīgām tehniskajām specifikācijām un procedūrām regulatīvās informācijas apstrādei un saziņai ar uzņēmējiem saistībā ar minēto informāciju.

(2) Lai noteiktu minētās kopīgās procedūras un noteikumus saskaņā ar Regulas (ES) 2020/1056 8. pantu, Komisijai būtu jāuzskaita galvenie *eFTI* apmaiņas vides informācijas un komunikācijas tehnoloģiju (“IKT”) komponenti, kas dalībvalstīm jānodrošina, un sīki jāizklāsta to funkcionālās un tehniskās specifikācijas.

(3) Lai minēto kopīgo procedūru un sīki izstrādāto noteikumu piemērošanā nodrošinātu elastību, dalībvalstīm jābūt iespējai izlemt, kā organizēt IKT komponentu nodrošināšanu, ja vien minētie komponenti atbilst attiecīgajām funkcionālajām un tehniskajām specifikācijām, kas noteiktas šajā regulā. Konkrētāk, dalībvalsts var pieņemt lēmumu tos izveidot kā atsevišķus komponentus vai integrēt vienā komponentā vai vairākos atsevišķos komponentos, kas nodrošina attiecīgās funkcijas. Tās var arī izveidot vairākus komponentus, kas nodrošina vienu un to pašu funkciju kopumu.

(4) Dalībvalstīm jābūt iespējai atkalizmantot tos IKT komponentus, ko tās ir izstrādājušas citiem digitālajiem publiskajiem pakalpojumiem, ciktāl šie komponenti jau nodrošina vajadzīgās funkcijas – vai tiek pielāgoti šo funkciju nodrošināšanai – saskaņā ar specifikācijām, attiecīgā gadījumā arī tehniskajām prasībām, kuras noteiktas šajā regulā. Dalībvalstīm jābūt arī iespējai izvēlēties izveidot, izstrādāt un uzturēt vienu vai vairākus šajā regulā paredzētos IKT komponentus kopīgi ar citām dalībvalstīm.

(5) Katrai dalībvalstij jāatbild par to, lai tiktu nodrošināta to IKT komponentu uzturēšana un drošība, kurus tā izveidojusi vai par kuriem tā atbild, tai skaitā par minētajos komponentos apstrādātās informācijas drošības un konfidencialitātes nodrošināšanu. Ja vairākas dalībvalstis nolemj kādu no minētajiem komponentiem izveidot un pārvaldīt kopīgi, tām būtu jānodrošina, ka to attiecīgie pienākumi ir noteikti atbilstīgos nolīgumos vai vienošanās memorandos.

(6) Saskaņā ar Regulu (ES) 2020/1056 visai saziņai *eFTI* apmaiņas vidē jānotiek, izmantojot drošus savienojumus starp pienācīgi identificētām un pilnvarotām personām. Tāpēc šajā regulā noteiktajām kopīgajām funkcionālajām un tehniskajām specifikācijām būtu jānodrošina, ka šādas prasības tiek izpildītas attiecībā uz visu saziņu, kas notiek starp *eFTI* apmaiņas vides dalībniekiem, izmantojot IKT komponentus, tostarp ar *eFTI* platformām.

([1]) OV L 249, 31.7.2020., 33. lpp.

(7) Paredzams, ka dalībnieku skaits *eFTI* apmaiņas vidē būs liels gan kompetento iestāžu līmenī, gan tādu attiecīgo uzņēmēju līmenī, kuri varēs brīvi izmantot *eFTI* platformas pēc savas izvēles. Tādēļ starp *eFTI* apmaiņas vides IKT komponentiem būtu jāizveido un jāuztur pietiekams skaits drošu, autentificētu un atļautu savienojumu. Lai samazinātu izmaksas, kas saistītas ar tik lielu savienojumu skaitu, dažiem *eFTI* apmaiņas vides IKT komponentiem, kas dalībvalstīm jāizveido, šajā apmaiņā būtu jānodrošina starpniecība, pildot vārtejas funkciju un vienlaikus saglabājot augstu drošības līmeni un piemērojamo atļauju ievērošanu.

(8) Tādām vārtejām jeb "*eFTI* vārtiem" jābūt par starpnieku regulatīvās kravu pārvadājumu informācijas apmaiņā starp attiecīgajiem uzņēmējiem un kompetentajām iestādēm. *eFTI* vārtiem jānodrošina droši un autentificēti savienojumi ar IKT komponentiem, kas ir starpnieki atsevišķu darbinieku piekļuvei konkrētas dalībvalsts kompetento iestāžu līmenī, no vienas puses, un *eFTI* platformām, kuru rīcībā ir dati, kuriem šiem darbiniekiem vajadzīga piekļuve, no otras puses. Tiem nav jāglabā vai jāapstrādā *eFTI* dati, izņemot metadatus, kas saistīti ar *eFTI* datu apstrādi, kā identifikatori vai darbības žurnāli, un tikai leģitīmiem mērķiem, kā maršrutēšana, formāta validēšana vai pielāgošana, un uzraudzība vai statistika.

(9) Turklāt, lai samazinātu ar savienojumu izveidi starp *eFTI* platformām un *eFTI* vārtiem saistītās izmaksas, sevišķi uzņēmējiem, taču arī kompetentajām iestādēm, kā paredzēts Regulas (ES) 2020/1056 8. panta 2. punktā, *eFTI* platformām būtu jāizveido un jāuztur drošs un autentificēts savienojums tikai ar vieniem *eFTI* vārtiem. Pēc tam minētajiem *eFTI* vārtiem būtu jāpilda starpnieka funkcija savienojuma nodrošināšanā visām kompetentajām iestādēm visās dalībvalstīs, izmantojot drošu un autentificētu savienojumu tīklu starp dažādajiem *eFTI* vārtiem.

(10) Ņemot vērā Regulas (ES) 2020/1056 11. pantā noteikto prasību, ka dalībvalstīm ir regulāri jāatjaunina to *eFTI* platformu saraksts, kurām ir derīgs sertifikāts, ko izdevusi to dalībvalstī akreditēta atbilstības novērtēšanas struktūra, šis vienotais *eFTI* platformas savienojums ar *eFTI* vārtu tīklu būtu jāizveido ar tās dalībvalsts *eFTI* vārtiem, kurā izdots minētās platformas sertifikāts. Tas atvieglotu un padarītu lētāku *eFTI* platformas sertifikācijas derīguma pārbaudes procesu, kas ir daļa no saziņas ar *eFTI* platformu drošības un autentiskuma nodrošināšanas procesa. Tomēr, lai pielāgotos situācijām, kad kādā dalībvalstī neviena atbilstības novērtēšanas struktūra nav akreditēta *eFTI* platformu sertificēšanai, *eFTI* platformām jābūt iespējai izveidot savu vienoto savienojumu ar šādas dalībvalsts *eFTI* vārtiem pat tad, ja tās sertifikātu saņēmušas citās dalībvalstīs.

(11) Lai nodrošinātu augstu uzticēšanās līmeni *eFTI* apmaiņas videi, dalībvalstīm arī turpmāk būtu jāatbild par to, lai visa to kompetento iestāžu piekļuve *eFTI* apmaiņas videi tiktu pienācīgi identificēta, autentificēta un atļauta. Dalībvalstīm būtu jānodrošina, ka piekļuve datiem, ko uzņēmēji darījuši pieejamus *eFTI* platformās, un to apstrāde kompetentajām iestādēm ir atļauta tikai pēc atbildīgo darbinieku pienācīgas identifikācijas un autentifikācijas, kā arī pēc pienācīgas atļaujas saņemšanas, pamatojoties uz darbiniekiem piešķirtajām piekļuves un apstrādes tiesībām un viņu attiecīgajiem pienākumiem saistībā ar ES un valstu noteikumiem, uz kuriem attiecas Regulas (ES) 2020/1056 darbības joma. Šajā nolūkā dalībvalstīm būtu jānodrošina, ka visas kompetentās iestādes izveido un uztur reģistrus, kuros glabā atjauninātus ierakstus par katra atbildīgā darbinieka piekļuves un apstrādes tiesībām, un ka visos pieprasījumos piekļūt *eFTI* datiem un tos apstrādāt ir iekļautas atsauces uz darbinieka, kas atbild par pieprasījumu, piekļuves un apstrādes tiesībām. Minētās piekļuves un apstrādes tiesības būtu jāizsaka kodētu atsauču veidā, lai līdz minimumam samazinātu darbinieku persondatu nosūtīšanu, kā noteikts Eiropas Parlamenta un Padomes Regulā (ES) 2016/679 ([2]). Dalībvalstīm arī būtu jānodrošina, ka to kompetentās iestādes veic visus pasākumus, piemēram, testēšanu, mācības un revīzijas, kas vajadzīgi, lai nodrošinātu, ka to darbinieki piekļūst datiem un apstrādā tos saskaņā ar piemērojamiem ES un valsts noteikumiem par datu privātumu un komerciālo konfidencialitāti.

([2]) Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.).

(12) Regulā (ES) 2020/1056 ir noteikts, ka attiecīgajiem uzņēmējiem ir jāpaziņo kompetentajām iestādēm "unikālā elektroniskā identifikācijas saite" uz mašīnlasāmajiem *eFTI* datiem, kas atbilst regulatīvajai informācijai. Procedūru ziņā šī saziņa būtu jāveic divējādi, un IKT komponentiem, kas dalībvalstīm jāizveido, būtu jāatbalsta abas procedūras. Kompetentajām iestādēm, pieprasot piekļuvi *eFTI* datiem, lai veiktu regulatīvās informācijas pārbaudes, vajadzētu būt iespējai izvēlēties kādu no procedūrām.

(13) Pirmkārt, saskaņā ar pašreizējām papīra formas atbilstības pārbaudes procedūrām attiecīgajiem uzņēmējiem jābūt iespējai tieši paziņot kompetentajai iestādei unikālo elektronisko identifikācijas saiti pārbaudēs, kas tiek veiktas fiziskā klātbūtnē vai nu pārvadājuma laikā, vai uzņēmēja telpās, ja attiecīgā gadījumā ES vai valsts noteikumi paredz iespēju veikt pārbaudes pēc pārvadāšanas darbību pabeigšanas. Lai kompetentajām iestādēm atvieglotu apstrādi, unikālā elektroniskā identifikācijas saite būtu jāpaziņo mašīnlasāmā formātā, piemēram, tāda svītrkoda vai kvadrātkoda veidā, kas redzams elektroniskas portatīvas ierīces, piemēram, mobilā tālruņa vai planšetdatora, ekrānā vai nodrukāts uz papīra. Dalībvalstu iestādēm jābūt iespējai izlemt, vai pieņemt to, ka situācijās, kad notiekošo pārvadājumu fizisko pārbaužu laikā uzņēmējs nav varējis tieši parādīt unikālo elektronisko identifikācijas saiti ekrānā vai uz papīra, viņš izņēmuma kārtā to var paziņot, izmantojot e-pastu vai citu elektronisku ziņapmaiņas lietotni. Attiecībā uz uzņēmēju telpās veiktajām pārbaudēm – ja inspicējamo pārvadājumu skaits ir ievērojami lielāks, kompetentajām iestādēm jābūt iespējai izvēlēties unikālo elektronisko identifikācijas saišu saņemšanu e-pastā vai citā elektroniskā ziņapmaiņas lietotnē, lai atvieglotu un optimizētu šo saišu apstrādi. Šo papildu saziņas līdzekļu izvēlei būtu jāpaliek attiecīgo kompetento iestāžu ziņā.

(14) Otrkārt, un saderīgāk ar nākotni, kur procesi ir vairāk automatizēti, uzņēmējiem būtu jāpaziņo unikālā elektroniskā identifikācijas saite, to publicējot elektroniskā repozitorijā vai reģistrā kopā ar noteiktiem identifikatoriem, piemēram, transportlīdzekļa unikālo identifikāciju, kas iegūta no *eFTI* datu kopas, kura saistīta ar minēto unikālo elektronisko identifikācijas saiti. Pēc tam kompetentās iestādes varētu izgūt šo saiti no reģistra ar vaicājumu, kas pamatots uz šajos identifikatoros. Tas ļautu kompetentajām iestādēm pārbaudīt informāciju par kravas automobilī, vilcienā vai liellaivā pārvadātajām precēm, transportlīdzekli fiziski neapturot vai tajā neiekāpjot, un attiecīgā gadījumā piemērot turpmākus pasākumus saskaņā ar valsts tiesību aktiem. Tas arī ļautu kompetentajām iestādēm saskaņā ar Eiropas Parlamenta un Padomes Regulas (EK) Nr. 1072/2009 ([3]) noteikumiem vieglāk vai ticamāk izgūt informāciju par vairākiem pārvadājumiem, kas veikti ar konkrētu transportlīdzekli konkrētā laikposmā, piemēram, kabotāžas autopārvadājumu pārbaužu gadījumā.

(15) Lai nodrošinātu sadarbspēju un drošību informācijas apmaiņā starp *eFTI* vārtiem, ko izveidojušas dažādās dalībvalstis, un starp *eFTI* vārtiem un *eFTI* platformām, *eFTI* vidē būtu jāizmanto saskaņotu standartu un specifikāciju kopums attiecībā uz ziņojumu apmaiņu, ieskaitot ziņojumu apmaiņas nolīgumu, uzņēmējdarbības procesu, datu formātu, identifikatoru un drošības sertifikātu konfigurāciju. Dalībvalstīm arī būtu jāvienojas par drošām procedūrām drošības sertifikātu apmaiņai, piemēram, izmantojot īpaši izveidotu sistēmu vai drošu datņu pārsūtīšanas protokolu.

(16) Lai samazinātu izmaksas un laiku, kas vajadzīgs, lai izveidotu *eFTI* vārtus un citus IKT komponentus, dalībvalstīm pēc iespējas būtu jāpaļaujas uz atvērtiem standartiem, ko uztur Eiropas vai starptautiskās organizācijas, un uz atkalizmantojamiem risinājumiem. Attiecībā uz ziņojumu apmaiņas formātiem visplašāk izmantotie starptautiski atzītie atvērtie standarti ir *XML* un *JSON*. Lai gan *JSON* ir jaunāks un dažos aspektos vienkāršāk īstenojams formāts, *XML* ir visizplatītākais formāts, ko kompetento iestāžu IKT sistēmās izmanto vairums dalībvalstu. Tāpēc, lai dalībvalstis varētu atkalizmantot pastāvošos risinājumus un tādējādi samazināt savas sākotnējās īstenošanas izmaksas, visai saziņai starp *eFTI* vārtiem un starp *eFTI* vārtiem un *eFTI* platformām būtu jānotiek, izmantojot vienotu ziņojumu apmaiņas formātu – *XML*. Līdzīgi drošas ziņojumu apmaiņas standarti, ko Komisija uztur kā daļu no *eDelivery* digitālā pamatelementa ([4]), jo īpaši *eDelivery* AS4 profils, nodrošina izmaksu ziņā efektīvu tehnisko risinājumu, kura īstenošanā dalībvalstīm jau ir pieredze.

([3]) Eiropas Parlamenta un Padomes Regula (EK) Nr. 1072/2009 (2009. gada 21. oktobris) par kopīgiem noteikumiem attiecībā uz piekļuvi starptautisko kravas autopārvadājumu tirgum (OV L 300, 14.11.2009., 72. lpp.).

([4]) https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eDelivery.

(17) Vienlaikus dalībvalstīm papildus *eDelivery* vajadzētu būt iespējai atkalizmantot ziņojumu apmaiņas standartus un risinājumus, ko jau izmanto citiem digitālajiem publiskajiem pakalpojumiem, saziņai starp *eFTI* vārtiem un *eFTI* platformām, kuras izveidotas attiecīgajā dalībvalstī. Minēto risinājumu pamatā esošās sīki izstrādātās prasības un standarti būtu jādara publiski pieejami, lai ieinteresētie *eFTI* platformu izstrādātāji tos varētu īstenot un lai akreditētās atbilstības novērtējuma struktūras varētu novērtēt to atbilstību specifikācijām.

(18) Līdzīgi, lai kompetento iestāžu darbinieki varētu izmantot IKT komponentus, kas veido piekļuves punktu vai "iestāžu piekļuves punktus" *eFTI* videi, dalībvalstīm vajadzētu būt iespējai izmantot pastāvošos elektroniskos risinājumus, kuri nodrošina darbinieku identificēšanu un identitātes autentificēšanu, kad viņi piekļūst citiem valsts digitālajiem publiskajiem pakalpojumiem, kas nodrošina piekļuvi trešo personu persondatiem vai komercdatiem. Šiem risinājumiem, ja tādi pieejami, būtu jābalstās uz elektroniskās identifikācijas līdzekļiem, kas noteikti Eiropas Parlamenta un Padomes Regulā (ES) Nr. 910/2014 ([5]).

(19) Tāpat dalībvalstīm vajadzētu būt iespējai atkalizmantot jebkurus citus pastāvošus to kompetento iestāžu IKT sistēmu komponentus, kuru veiktās funkcijas ir līdzīgas šajā regulā noteiktajām funkcijām, piemēram, atļauju reģistrus, ja vien tie ir pielāgoti šajā regulā noteiktajām īpašajām prasībām.

(20) Lai kompetento iestāžu darbiniekiem būtu pēc iespējas vienkāršāk izmantot *eFTI* apmaiņas vidi un lai atvieglotu to *eFTI* datu analīzi, kurus uzņēmēji darījuši pieejamus *eFTI* platformā, dalībvalstīm jābūt iespējai pielāgot lietotāja lietotni un tās grafisko lietotāja saskarni savu darbinieku vajadzībām. Ja dalībvalstis vēlētos, tām jābūt arī iespējai ieviest papildu funkcijas, kas jāatbalsta ar lietotāju lietotnēm, piemēram, tādu viedo algoritmu izmantošanu, kuri var iepriekš apstrādāt *eFTI* datus, arī apvienojot informāciju no citiem elektroniskiem avotiem.

(21) Lai *eFTI* vide darbotos nepārtraukti un netraucēti, ir ātri jāatrisina visas darbības problēmas, kas saistītas ar dalībvalstu izveidotajiem IKT komponentiem. Lai to palīdzētu nodrošināt, dalībvalstīm un Komisijai būtu jāizveido tehniskā atbalsta tīkls, kas sastāvētu no specializētiem palīdzības dienestiem valsts un attiecīgi Savienības līmenī. Attiecībā uz šo tīklu būtu jāizveido skaidras saziņas procedūras un jānodrošina sinhronizēti minimālie pieejamības periodi, lai varētu ātri reaģēt uz jebkādiem iespējamiem incidentiem un dīkstāvēm, kas var ietekmēt *eFTI* apmaiņas vides darbību. Lai minētie tehniskā atbalsta kontaktpunkti varētu veikt savus uzdevumus, tiem vajadzīgas pilnvaras un pietiekami cilvēkresursi un finanšu resursi. Pamatojoties uz darbības pārskatiem, palīdzības dienesti var publicēt apkopotu informāciju īpašos palīdzības dienesta infopaneļos. Palīdzības dienestu kopējās pieejamības minimālie periodi būtu periodiski jāpārskata, lai varētu pielāgot to darbību un efektīvi sadalīt resursus.

(22) IKT komponenti, kas dalībvalstīm jāizveido, darbosies kā plašākas *eFTI* apmaiņas vides sastāvdaļa. Tas nozīmē, ka šie komponenti būtu koordinēti jāizveido un jāuztur, pamatojoties uz šajā regulā noteikto specifikāciju saskaņotu interpretāciju. Šajā nolūkā dalībvalstīm sadarbībā ar Komisiju būtu jāizveido arī operatīvā atbalsta tīkls īpašas ekspertu grupas veidā. Lai izmantotu zināšanas un pieredzi, kas gūta Digitālajā transporta un loģistikas forumā (DTLF) – ekspertu grupā, ko Komisija izveidojusi ([6]), lai palīdzētu izstrādāt un īstenot Savienības darbības un programmas, kuru mērķis ir transporta un loģistikas nozares digitalizācija, – minētā ekspertu grupa būtu jāizveido kā DTLF apakšgrupa.

(23) Lai atvieglotu dalībvalstu īstenošanas centienus un nodrošinātu šo specifikāciju vienādu īstenošanu, šo regulu ir paredzēts papildināt ar sīkāk izstrādātiem nesaistošiem tehniskā atbalsta dokumentiem, ko Komisija sagatavojusi sadarbībā ar dalībvalstīm minētajā īpašajā ekspertu grupā.

([5]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 (2014. gada 23. jūlijs) par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK (OV L 257, 28.8.2014., 73. lpp.).

([6]) Komisijas Lēmums C(2018) 5921 (2018. gada 13. septembris), ar ko izveido kravu pārvadājumu un loģistikas digitalizācijas ekspertu grupu: Digitālo transporta un loģistikas forumu (DTLF).

(24) Šajā regulā paredzētie pasākumi ir saskaņā ar Digitālā transporta un tirdzniecības veicināšanas komitejas atzinumu,

IR PIEŅĒMUSI ŠO REGULU.

I NODAĻA

VISPĀRĪGIE NOTEIKUMI

1. pants

Definīcijas

Šajā regulā piemēro šādas definīcijas:

1) "*eFTI* apmaiņas vide" ir IKT komponentu kopums, ko izmanto datu apmaiņai saskaņā ar Regulu (ES) 2020/1056, kā arī atbilstīgi šai regulai pieņemtajiem īstenošanas un deleģētajiem aktiem;

2) "IKT komponents" ir materiāla (aparatūras) vai nemateriāla (programmatūras) vienība vai tādu vienību kopums, ko izmanto īpašu funkciju veikšanai, lai nodrošinātu datu elektronisku pārraidi;

3) "kompetentās iestādes darbinieks" ir fiziska persona, kas dalībvalsts kompetentās iestādes vārdā ir tiesīga piekļūt Regulas (ES) 2020/1056 2. panta 1. punktā minētajām regulatīvās informācijas prasībām un apstrādāt šo informāciju;

4) "*eFTI* dati" ir dati, kas atbilst regulatīvajai informācijai, ko uzņēmēji darījuši pieejamu *eFTI* platformā saskaņā ar Regulu (ES) 2020/1056;

5) "pieprasījums piekļūt *eFTI* datiem" ir kompetentās iestādes vārdā izteikts pieprasījums saņemt *eFTI* datus, ko uzņēmēji darījuši pieejamus *eFTI* platformā;

6) "papildu paziņojums" ir saziņa starp kompetentajām iestādēm un attiecīgajiem uzņēmējiem par informāciju, ko uzņēmēji darījuši pieejamu *eFTI* platformā, pēc tam kad kompetentās iestādes darbinieks veicis minētās informācijas atbilstības pārbaudi, atbildot uz pieprasījumu piekļūt *eFTI* datiem. Šajā papildu paziņojumā var tikt pieprasīts sniegt trūkstošos *eFTI* datus vai informāciju par turpmākiem pasākumiem, ko kompetentā iestāde veikusi saskaņā ar piemērojamajiem valsts noteikumiem;

7) "piekļuves tiesības" ir atļaujas, kas piešķirtas kompetentās iestādes darbiniekam darbībām, kas saistītas ar vienu vai vairākām *eFTI* datu apakškopām;

8) "apstrādes tiesības" ir darbības vai darbību kopumi, ko kompetentās iestādes darbiniekam atļauts veikt attiecībā uz konkrētu *eFTI* datu apakškopu, kura saņemta, atbildot uz pieprasījumu piekļūt *eFTI* datiem;

9) "elektroniskās identifikācijas līdzekļi" ir materiāli vai nemateriāli elementi, kas ietver personas identifikācijas datus un ko izmanto, lai autentificētos tiešsaistes pakalpojumam;

10) "identifikācijas dati" ir personas identifikācijas numurs vai kodēta atsauce, kas nodrošina kompetentās iestādes darbinieka unikālu identificēšanu;

11) "iestādes piekļuves punkts (IPP)" ir IKT komponents vai IKT komponentu kopums, kas nodrošina 4. pantā izklāstītās funkcijas;

12) "*eFTI* vārti" ir IKT komponents vai IKT komponentu kopums, kas nodrošina 6. pantā izklāstītās funkcijas;

13) "pieprasītājvārti" ir *eFTI* vārti, kas apstrādā *eFTI* datu piekļuves pieprasījumu, kurš iesniegts, izmantojot IPP, kas savienots ar minētajiem *eFTI* vārtiem vai tajos integrēts;

14) "saņēmējvārti" ir *eFTI* vārti, kas apstrādā *eFTI* datu piekļuves pieprasījumu, kurš saņemts no pieprasītājvārtiem;

15) "*eDelivery*" ir elektroniskās ziņojumu apmaiņas tehnisko specifikāciju un standartu kopums, ko Komisija izstrādājusi Eiropas infrastruktūras savienošanas instrumenta programmā ([7]) un turpina programmā "Digitālā Eiropa" ([8]);

16) "*eDelivery* piekļuves punkts" ir saziņas komponents, kurš ir daļa no *eDelivery* elektroniskās piegādes pakalpojuma un kura pamatā ir tehniskās specifikācijas un standarti;

17) "statiska atklāšana" ir mehānisms, ar kura palīdzību *eDelivery* piekļuves punkts iegūst cita *eDelivery* piekļuves punkta savienojuma informāciju, neizmantojot trešu personu sistēmas;

18) "dinamiska atklāšana" ir mehānisms, ar kura palīdzību *eDelivery* piekļuves punkts iegūst savienojuma informāciju par citu *eDelivery* piekļuves punktu, meklējot šos datus trešas personas sistēmā;

19) "drošības atslēgas" ir publisko un privāto šifrēšanas atslēgu pāri, ko ļoti lielu numuru veidā ģenerē šifrēšanas algoritmi un kam ir unikālas savstarpējas attiecības;

20) "drošības sertifikāts" ir sertificētājas iestādes izdots digitāls dokuments, ko izmanto, lai izveidotu drošu elektronisko sakaru kanālu starp divām pusēm; tas ietver publisko drošības atslēgu un informāciju par sertifikāta priekšmetu;

21) "sertificētāja iestāde" ir struktūra, kura pārvalda digitālo sertifikātu aprites ciklu, kas var ietvert reģistrācijas procesus un drošības sertifikātu izdošanas, piegādes, aktivizēšanas, apturēšanas, atsaukšanas, atjaunošanas vai atkārtotas aktivizēšanas procesus;

22) "lietotāja lietotne" ir IKT komponents, kas nodrošina 7. pantā izklāstītās funkcijas;

23) "tehnisko norādījumu dokuments" ir sīki izstrādātu un nesaistošu tehnisko dokumentu kopums, ko Komisija sagatavojusi sadarbībā ar dalībvalstīm 13. pantā minētajā darba grupā.

2. pants

Kopīgi pasākumi

1. Dalībvalstis nodrošina, ka to kompetentajām iestādēm ir piekļuve IKT sistēmām, kuras var apstrādāt unikālās elektroniskās identifikācijas saites (UIS), ko uzņēmēji paziņojuši saskaņā ar Regulas (ES) 2020/1056 4. panta 3. punktu, un kuras ļauj to kompetento iestāžu darbiniekiem piekļūt *eFTI* datiem un tos apstrādāt, veicot kādu no šīm procedūrām:

a) tieši apstrādājot UIS, ja uzņēmējs to paziņo mašīnlasāmā formā, izvietojot elektroniskas ierīces ekrānā vai izdrukājot uz fiziska pamata, piemēram, papīra, vai, ja kompetentā iestāde pieļauj šādu saziņu, arī nosūtot to e-pastā vai citādā elektroniskas ziņojumapmaiņas lietotnē;

b) vispirms izgūstot UIS, ko uzņēmēji paziņojuši, publicējot īpašā reģistrā, izmantojot unikālu identifikatoru, kas saistīts ar pārvadājumu.

2. Dalībvalstis nodrošina, ka 1. punktā minētajām IKT sistēmām ir vismaz šādas funkcijas:

a) kompetento iestāžu darbinieku pienācīgi autentificēta identifikācija un pienācīga atļaujas saņemšana ikreiz, kad darbinieks iesniedz pieprasījumu piekļūt *eFTI* datiem;

b) starpniecības nodrošināšana saistībā ar kompetento iestāžu darbinieku iesniegtajiem pieprasījumiem piekļūt *eFTI* datiem, arī izgūt pieprasīto informāciju no attiecīgās *eFTI* platformas vai platformām, izmantojot drošus savienojumus ar minētajām platformām.

([7]) https://digital-strategy.ec.europa.eu/lv/activities/cef-digital.
([8]) https://digital-strategy.ec.europa.eu/lv/activities/digital-programme.

3. Lai īstenotu 2. punktā uzskaitītās funkcijas, minētajās IKT sistēmās ir vismaz šādi komponenti:

a) iestāžu piekļuves punkti (IPP);

b) atļauju reģistrs;

c) *eFTI* vārti;

d) meklēšanas mehānisms;

e) lietotāja lietotne.

4. Dalībvalstis nodrošina, ka 3. punktā uzskaitītie komponenti atbilst II nodaļā noteiktajām prasībām. Dalībvalstis atbild par minēto komponentu izveidi, mitināšanu, izstrādi, pieejamību, uzraudzību, atjaunināšanu un uzturēšanu, kā arī par minētajos komponentos apstrādātās informācijas drošību. Ja divas vai vairākas dalībvalstis vienu vai vairākus minētos komponentus izveido vai izstrādā kopīgi, tās kopīgi atbild par to izveidi, mitināšanu, izstrādi, pieejamību, uzraudzību, atjaunināšanu, uzturēšanu un drošību.

5. Dalībvalstis joprojām atbild par to, lai nodrošinātu, ka kompetento iestāžu piekļuve *eFTI* datiem un to apstrāde tiek veikta tikai nolūkā pārbaudīt atbilstību piemērojamām ES un valsts tiesību normām un saskaņā ar piemērojamiem ES un valsts noteikumiem, kuros paredzēti nosacījumi minēto atbilstības pārbaužu veikšanai, un noteikumiem par persondatu privātuma un komercdatu konfidencialitātes ievērošanu.

3. pants

Pieprasījumi piekļūt *eFTI* datiem, atbildes un papildu paziņojums

1. Kompetento iestāžu darbinieki visus pieprasījumus piekļūt *eFTI* datiem iesniedz, izmantojot 4. pantā aprakstīto IPP komponentu un 7. pantā aprakstīto lietotni.

2. Pieprasījumā piekļūt *eFTI* datiem ietver šādu informāciju:

a) to *eFTI* datu UIS, kuriem pieprasīta piekļuve, vai vienu vai vairākus identifikatorus, kas ļauj UIS izgūt no 11. pantā aprakstītā identifikatoru reģistra. Šo informāciju sniedz par pieprasījumu atbildīgais kompetentās iestādes darbinieks;

b) atsauces uz kompetentās iestādes darbinieka, kurš atbild par pieprasījuma iesniegšanu, piekļuves tiesībām, kas reģistrētas 5. pantā aprakstītajā atļauju reģistrā. Šai informācijai lietotāja lietotnē jātiek pievienotai automātiski;

c) pieprasījuma unikālo identifikācijas numuru, ko izdevis IPP. Šai informācijai lietotāja lietotnē jātiek pievienotai automātiski.

3. Atbildes uz pieprasījumu piekļūt *eFTI* datiem var tikt sniegtas kādā no šādiem veidiem:

a) *eFTI* dati, ko nosūta *eFTI* platforma, pamatojoties uz pieprasījumā ietverto informāciju, un saistītie ziņojumu apmaiņas metadati vai identifikatori, kas vajadzīgi, lai *eFTI* saņēmējvārti vai iestāžu piekļuves punkti varētu kartēt *eFTI* datus attiecīgajam pieprasījumam;

b) kļūdu ziņojumi, kas ietver kodētu vai īsu tekstuālu precizējumu par kļūdas veidu, ja *eFTI* vārti vai *eFTI* platforma tehnisku vai ar uzņēmējdarbības procesu saistītu iemeslu dēļ nevar sniegt pieprasītos *eFTI* datus;

c) ziņojums, kurā norādīts, ka dati nav pieejami, un kuru izdod *eFTI* saņēmējvārti, kad tie apstrādā pieprasījumu, kurā ietverti identifikatori, un vārtu meklēšanas mehānisms savā identifikatoru reģistrā neatrod aktīvu UIS, kas saistīts ar šiem identifikatoriem;

d) ziņojums "nav atbildes", ko nosūta *eFTI* vārti vai *eFTI* platforma, ja minētie *eFTI* vārti vai platforma apstiprinājuši pieprasījuma saņemšanu, bet pēc saņemšanas apstiprinājuma nav 60 sekundēs nosūtījuši ziņojumu ar pieprasītajiem *eFTI* datiem.

4. Ja kompetentās iestādes darbinieks konstatē, ka informācija, ko uzņēmējs darījis pieejamu *eFTI* platformā un kas izgūta, atbildot uz pieprasījumu piekļūt *eFTI* datiem, ir nepilnīga vai citādi neatbilst regulatīvās informācijas prasībām, uz kuru pamata iesniegts pieprasījums, darbinieks šos konstatējumus var paziņot uzņēmējam, iesniedzot īpašu papildu paziņojumu par minēto informāciju. Tādā papildu paziņojumā ievēro piemērojamās valsts tiesību aktu prasības par regulatīvās atbilstības pārbaužu turpmākajiem pasākumiem.

5. Ja tiek iesniegts īpašs papildu paziņojums, kas minēts 4. punktā, kompetentā iestāde, izmantojot lietotāja lietotni, to nosūta arī IPP komponentā. Tajā ietver:

a) informāciju, ko kompetentā iestāde paredzējusi paziņot uzņēmējam, brīvā teksta formā vai pievienota dokumenta veidā;

b) *eFTI* datu UIS un tā pieprasījuma unikālo identifikācijas numuru, kas attiecas uz piekļuvi šiem datiem, par kuriem sniegts papildu paziņojums.

II NODAĻA

FUNKCIONĀLIE KOMPONENTI

4. pants

Iestāžu piekļuves punkti

1. IPP komponenti nodrošina kompetento iestāžu darbinieku piekļuvi *eFTI* apmaiņas videi, un tie ir darbinieka vienīgais piekļuves punkts šai videi.

2. IPP nodrošina šādas funkcijas:

a) autentificē kompetento iestāžu darbinieku identitāti vai nodrošina kompetento iestāžu darbinieku identitātes autentifikāciju;

b) apstiprina kompetento iestāžu darbinieku pieprasījumu piekļūt *eFTI* datiem, pamatojoties uz viņu attiecīgajām piekļuves tiesībām, kas norādītas atļauju reģistrā, vai noraida pieprasījumu, ja kompetentās iestādes darbiniekam nav reģistrētu aktīvu piekļuves tiesību;

c) reģistrē atļautos pieprasījumus piekļūt *eFTI* datiem, katram šādam pieprasījumam piešķirot unikālu identifikācijas numuru un par katru pieprasījumu reģistrējot vismaz šādu informāciju:

   i) par pieprasījuma iesniegšanu atbildīgā darbinieka identifikācijas dati;

   ii) to *eFTI* datu UIS, kuriem pieprasīta piekļuve, vai identifikators vai identifikatori, ko darbinieks norādījis, iesniedzot pieprasījumu;

   iii) atsauces uz kompetentās iestādes darbinieka, kurš atbild par pieprasījuma iesniegšanu, piekļuves tiesībām, kas reģistrētas atļauju reģistrā;

   iv) pieprasījuma iesniegšanas datums un laiks;

d) atļautos pieprasījumus piekļūt *eFTI* datiem nosūta *eFTI* vārtiem apstrādei, sniedzot šādu informāciju:

   i) pieprasījuma unikālais identifikācijas numurs;

   ii) to *eFTI* datu UIS, kuriem pieprasīta piekļuve, vai identifikators vai identifikatori, ko darbinieks norādījis, iesniedzot pieprasījumu;

   iii) atsauces uz kompetentās iestādes darbinieka, kas atbild par pieprasījuma iesniegšanu, apstrādes tiesībām, kas reģistrētas atļauju reģistrā;

e) saņem atbildes uz *eFTI* vārtu nosūtītajiem pieprasījumiem un, izmantojot lietotni, dara šīs atbildes pieejamas par minēto pieprasījumu atbildīgajam kompetentās iestādes darbiniekam;

f) saglabā revīzijas liecības par atbildēm, kas saņemtas par katru pieprasījumu, reģistrējot vismaz šādu informāciju:

i) tā pieprasījuma unikālais identifikācijas numurs, attiecībā uz kuru saņemta atbilde;

ii) datums un laiks, kad atbildi saņēmis IPP;

iii) datums un laiks, kad IPP pārsūtījis atbildi darbiniekam, kurš atbild par attiecīgo pieprasījumu;

g) glabā arhīvu ar *eFTI* datu piekļuves pieprasījumiem un saņemto atbilžu reģistru divus gadus vai, ja piemērojamie valsts noteikumi par pierādījumu pieejamību to noteikumu izpildes nodrošināšanai, attiecībā uz kuriem vajadzīga piekļuve *eFTI* datiem, paredz ilgāku laikposmu, – attiecīgo laikposmu;

h) ja tiek iesniegts papildu paziņojums saskaņā ar 3. panta 4. punktu, reģistrē šo papildu paziņojumu, piešķirot tam unikālu identifikācijas numuru, un par minēto papildu paziņojumu reģistrē vismaz šādu informāciju:

i) par papildu paziņojuma iesniegšanu atbildīgā darbinieka identifikācijas dati;

ii) *eFTI* datu UIS un tā pieprasījuma unikālais identifikācijas numurs, kas attiecas uz piekļuvi šiem datiem, par kuriem sniegts papildu paziņojums;

iii) papildu paziņojuma iesniegšanas datums un laiks;

iv) papildu paziņojuma saturs;

i) nosūta papildu paziņojumus *eFTI* vārtiem apstrādei, sniedzot šādu informāciju:

i) *eFTI* datu UIS un tā pieprasījuma unikālais identifikācijas numurs, kas attiecas uz piekļuvi šiem datiem, par kuriem sniegts papildu paziņojums;

ii) papildu paziņojuma saturs.

3. Lai nodrošinātu 2. punktā noteiktās funkcijas, IPP:

a) izmanto piemērotus elektroniskās identifikācijas līdzekļus, kas ļauj uzticami identificēt un autentificēt kompetento iestāžu darbiniekus vai kas ļauj pārbaudīt, vai minēto darbinieku identifikāciju un autentifikāciju nodrošina cits piemērots IKT komponents;

b) izmanto atļauju reģistru;

c) izveido un uztur drošu savienojumu ar *eFTI* vārtiem;

d) atbalsta drošu savienojumu ar lietotāja lietotni.

4. Dalībvalstis var izveidot IPP vai nu ārpus *eFTI* vārtiem kā daļu no attiecīgo kompetento iestāžu pastāvošajām IKT sistēmām, vai integrētu ro attiecīgajos *eFTI* vārtos.

5. pants

Atļauju reģistrs

Dalībvalstis nodrošina, ka to kompetento iestāžu darbinieku tiesības piekļūt *eFTI* datiem un tos apstrādāt tiek reģistrētas un pastāvīgi atjauninātas atļauju reģistrā. Atļauju reģistrā par katru kompetentās iestādes darbinieku iekļauj vismaz šādu informāciju:

a) darbinieka unikālie identifikācijas dati;

b) attiecīgā darbinieka piekļuves tiesības, kas izteiktas kā to Savienības un valstu tiesību aktu atsauču saraksts, kuros paredzēts nodrošināt regulatīvo informāciju, attiecībā uz ko konkrētajam darbiniekam ir kompetence, un, konkrētāk, kā minētajiem noteikumiem atbilstošo *eFTI* datu apakškopu attiecīgo identifikatoru saraksts, kā noteikts Komisijas Deleģētās regulas (ES) 2024/2024 ([9]) pielikuma 3. un 4. iedaļā;

c) attiecīgā darbinieka apstrādes tiesības, kas izteiktas kā kodētas atsauces uz apstrādes darbībām, kuras darbiniekam ir tiesības veikt katrā no attiecīgajām *eFTI* datu apakškopām, saskaņā ar piemērojamiem Savienības vai valsts tiesību aktiem, kuros paredzēta minētā darbinieka kompetence;

d) ierakstu par izmaiņām minētā darbinieka piekļuves un apstrādes tiesībās.

6. pants

eFTI vārti

1. *eFTI* vārti tieši vai izmantojot savienojumu ar citiem *eFTI* vārtiem nodrošina, ka:

a) atļautie pieprasījumi piekļūt *eFTI* datiem tiek nosūtīti *eFTI* platformai un satur konkrēto pieprasīto informāciju;

b) par katru šādu pieprasījumu no attiecīgās *eFTI* platformas saņemtā atbilde tieši vai – attiecīgā gadījumā – izmantojot IPP tiek nosūtīta uz tā kompetentās iestādes darbinieka lietotāja lietotni, kas atbildīgs par minēto pieprasījumu, kā arī

c) pēc iesniegšanas *eFTI* platformai par minēto pieprasījumu tiek nosūtīts papildu paziņojums, kurā ietverti *eFTI* dati, par ko bijis iesniegts pieprasījums, un sniegtā atbilde.

2. *eFTI* vārti nodrošina šādas funkcijas:

a) validē pieprasījumu piekļūt *eFTI* datiem un papildu paziņojumu, ja tāds iesniegts, kādā no šiem veidiem:

i) ja tie darbojas kā "pieprasītājvārti" un IPP ir izveidots kā atsevišķs komponents ārpus *eFTI* vārtiem, pārbauda tā IPP drošības atslēgu, caur kuru iesniegts pieprasījums vai papildu paziņojums;

ii) ja tie darbojas kā "saņēmējvārti", pārbauda to *eFTI* vārtu drošības atslēgu, no kuriem tie saņēmuši pieprasījumu vai papildu paziņojumu;

iii) ja attiecīgo *eFTI* vārtu drošības atslēgas validācija neizdodas, nosūta kļūdas ziņojumu attiecīgi pieprasītājvārtiem, IPP vai kompetentās iestādes darbiniekam, kurš atbild par pieprasījumu vai papildu paziņojumu;

b) apstrādā piekļuves *eFTI* datiem pieprasījumu un papildu paziņojumu, ja tāds iesniegts, izmantojot meklēšanas mehānismu saskaņā ar 8. pantu, un, pamatojoties uz to, pārsūta pieprasījumu vai attiecīgā gadījumā papildu paziņojumu:

i) attiecīgajai *eFTI* platformai vai *eFTI* vārtiem, ja tie darbojas kā pieprasītājvārti;

ii) attiecīgajai *eFTI* platformai, ja tie darbojas kā saņēmējvārti;

c) saglabā revīzijas liecības par visiem *eFTI* datu piekļuves pieprasījumiem vai papildu paziņojumiem, ko tie apstrādājuši, reģistrējot vismaz šādu informāciju:

i) *eFTI* datu piekļuves pieprasījuma vai papildu paziņojuma unikālais identifikācijas numurs;

ii) tā IPP vai to *eFTI* pieprasītājvārtu identifikators, no kura(-iem) saņemts minētais pieprasījums vai papildu paziņojums;

iii) minētā pieprasījuma saņemšanas datums un laiks;

([9]) Komisijas deleģētā regula (ES) 2024/2024 (2024. gada 26. jūlijs), ar ko papildina Regulu (ES) 2020/1056, izveidojot *eFTI* kopīgo datu kopu un *eFTI* datu apakškopas (OV L, 2024/2024, 20.12.2024., ELI: http://data.europa.eu/eli/reg_del/2024/2024/oj).

d) validē atbildi, kas saņemta attiecībā uz to apstrādāto pieprasījumu, šādi:

i) ja atbildi saņem tieši no *eFTI* platformas, pārbauda *eFTI* platformas drošības atslēgu un sertifikācijas statusu, pamatojoties uz 3. punkta e) apakšpunktā minēto reģistru;

ii) ja atbildi saņem no *eFTI* saņēmējvārtiem, pārbauda minēto *eFTI* vārtu drošības atslēgu, pamatojoties uz 3. punkta f) apakšpunktā minēto reģistru;

iii) ja attiecīgo *eFTI* vārtu vai *eFTI* platformas drošības atslēgas validācija neizdodas, nosūta atbilstīgu kļūdas ziņojumu attiecīgi pieprasītājvārtiem, IPP vai tā kompetentās iestādes darbinieka lietotāja lietotnei, kas atbildīgs par pieprasījumu;

e) nosūta saņemto atbildi attiecībā uz pieprasījumu, ko tie apstrādājuši, apgrieztā secībā izmantojot to pašu ceļu, kas izmantots nosūtītajam pieprasījumam, attiecīgi:

i) *eFTI* pieprasītājvārtiem vai

ii) tieši vai ar IPP starpniecību – par minēto pieprasījumu atbildīgā kompetentās iestādes darbinieka lietotnei;

f) ja saņemts pieprasījuma saņemšanas apstiprinājums, bet 60 sekunžu laikā pēc minētā apstiprinājuma saņemšanas nav saņemta nekāda cita atbilde, nosūta ziņojumu "nav atbildes" attiecīgi pieprasītājvārtiem, IPP vai par pieprasījumu atbildīgā kompetentās iestādes darbinieka lietotnei;

g) saglabā revīzijas liecības par visām atbildēm uz to nosūtītajiem piekļuves pieprasījumiem, reģistrējot vismaz šādu informāciju:

i) *eFTI* datu kopas UIS, ko tie saņēmuši, atbildot uz minēto pieprasījumu;

ii) tās *eFTI* platformas vai *eFTI* saņēmējvārtu unikālais identifikācijas numurs, no kuriem tie saņēmuši atbildi;

iii) atbildes saņemšanas datums un laiks;

iv) ja atbilde nav saņemta – attiecīga norāde;

h) arhivē un revīzijas vajadzībām glabā c) un g) apakšpunktā minētos reģistrus divus gadus vai, ja valsts noteikumi par pierādījumu pieejamību to noteikumu izpildes nodrošināšanai, attiecībā uz kuriem vajadzīga piekļuve *eFTI* datiem, paredz ilgāku laikposmu, – attiecīgo laikposmu.

3. Lai nodrošinātu 2. punktā minētās funkcijas, *eFTI* vārti:

a) izmanto meklēšanas mehānismu saskaņā ar 8. pantu;

b) izveido un uztur drošu savienojumu ar IPP, kas nodrošina starpniecību attiecībā uz tās dalībvalsts kompetento iestāžu darbinieku piekļuvi *eFTI* apmaiņas videi, kura izveidojusi attiecīgos *eFTI* vārtus;

c) ja IPP ir izveidoti kā *eFTI* vārtu integrēti komponenti, izveido un uztur drošu savienojumu ar tās dalībvalsts kompetentās iestādes darbinieku lietotni vai lietotnēm, kura izveidojusi attiecīgos *eFTI* vārtus;

d) ja IPP ir izveidoti kā atsevišķi *eFTI* vārtu komponenti, izveido un uztur atjauninātu reģistru, kas satur minēto IPP unikālos identifikācijas numurus un drošības sertifikātus;

e) izveido un uztur drošu savienojumu ar visiem pārējiem *eFTI* vārtiem, kā arī atjauninātu reģistru, kas satur minēto *eFTI* vārtu unikālos identifikācijas numurus un drošības sertifikātus;

f) izveido un uztur drošu savienojumu ar visām *eFTI* platformām, kas saņēmušas sertifikāciju dalībvalstī vai dalībvalstīs, kuras izveidojušas attiecīgos *eFTI* vārtus, kā arī atjauninātu reģistru, kurā ietverti minēto *eFTI* platformu unikālie identifikācijas numuri, drošības atslēgas un sertifikācijas statuss;

g) spēj izmantot kopīgi definētus pakalpojumus vai artefaktus, piemēram, konfigurāciju, kļūdu kodus, taksonomiju vai kodu sarakstus *eFTI* apmaiņas vidē, ja par šiem pakalpojumiem vai artefaktiem ir panākta vienošanās 13. pantā minētajā operatīvā atbalsta tīklā.

4. Ja dalībvalstī nav akreditēta neviena atbilstības novērtējuma struktūra *eFTI* platformu sertificēšanai saskaņā ar Regulas (ES) 2020/1056 11. pantu, minētā dalībvalsts nodrošina, ka tās *eFTI* vārti izveido un uztur drošu savienojumu un atjauninātu reģistru, kā minēts 3. punkta f) apakšpunktā, attiecībā uz *eFTI* platformām, kas saņēmušas sertifikāciju no citās dalībvalstīs akreditētām atbilstības novērtējuma struktūrām. Minētā dalībvalsts to dara pēc uzņēmēja vai *eFTI* pakalpojumu sniedzēja, kas izmanto minēto platformu, pieprasījuma un pēc tam, kad tā pieprasījusi un saņēmusi apstiprinājumu no dalībvalsts, kurā *eFTI* platforma saņēmusi sertifikātu, par to, ka tā attiecībā uz to pašu *eFTI* platformu nav saņēmusi nevienu citu apstiprinājuma pieprasījumu no citas dalībvalsts. Tādējādi tās dalībvalsts *eFTI* vārti, kurā *eFTI* platforma saņēmusi sertifikātu, tiek atbrīvoti no pienākuma izveidot un uzturēt drošu savienojumu ar minēto platformu.

7. pants

Lietotāja lietotne

1. Lietotāja lietotne ļauj kompetentās iestādes darbiniekam mijiedarboties ar IPP.

2. Lietotāja lietotne nodrošina vismaz šādas funkcijas:

a) ģenerē pieprasījumus piekļūt *eFTI* datiem, pamatojoties uz kompetentās iestādes darbinieka sniegto informāciju, tiklīdz atbildīgais darbinieks ir pienācīgi identificēts, autentificēts un saņēmis IPP atļauju;

b) saņem un kompetentās iestādes darbiniekam, kas atbildīgs par pieprasījumu, parāda atbilstīgos *eFTI* datus, ko sniegusi(-šas) attiecīgā(-s) *eFTI* platforma(-s), atbildot uz minēto pieprasījumu, vai parāda ziņojumu "nav atbildes" vai kļūdu ziņojumus, ko pārsūtījis IPP vai "*eFTI* saņēmējvārti";

c) ļauj kompetentās iestādes darbiniekam, kas atbildīgs par saņemto *eFTI* datu pieprasījumu, veikt citas apstrādes darbības saskaņā ar minētā darbinieka apstrādes tiesībām;

d) ja to atļauj piemērojamie valsts noteikumi, ģenerē papildu paziņojumus, pamatojoties uz kompetentās iestādes darbinieka sniegto informāciju.

3. Lai nodrošinātu 2. punktā minētās funkcijas, lietotāja lietotne veic vismaz šādas darbības:

a) nodrošina kompetentās iestādes darbiniekiem grafisku lietotāja saskarni;

b) izveido un uztur drošu savienojumu attiecīgi ar IPP vai *eFTI* vārtiem;

c) attiecībā uz datu apstrādi – par atsauci izmanto datu apakškopas, kuras atbilst Savienības un valsts tiesību aktu noteikumiem, kā noteikts Komisijas Deleģētajā regulā (ES) 2024/2024, un attiecībā uz kurām kompetentajai iestādei ir kompetence.

8. pants

Meklēšanas mehānisms

1. Meklēšanas mehānisms ir *eFTI* vārtos integrēts komponents, kura galvenā funkcija ir pieprasījumā vai papildu paziņojumā iekļauto informāciju apstrādāt šādi:

a) no *eFTI* datu UIS izgūt tās *eFTI* platformas identifikatoru, kur tiek glabāti *eFTI* dati, attiecībā uz kuriem iesniegts piekļuves pieprasījums vai papildu paziņojums, un attiecīgi to *eFTI* vārtu identifikatoru, ar kuriem minētā platforma savienota;

b) ja informācijas pieprasījumā ir viens vai vairāki 11. panta 3. punktā noteiktie identifikatori, meklēt identifikatoru reģistrā atbilstošo vērtību un:

   i) ja tiek konstatēta atbilsme, izgūt aktīvo UIS vai UIS kopu, kas saistīta ar attiecīgajiem identifikatoriem, pēc tam apstrādāt informāciju attiecīgajās UIS saskaņā ar a) apakšpunktu;

   ii) ja atbilsme netiek atrasta, attiecīgi paziņot *eFTI* vārtiem.

2. Lai nodrošinātu 1. punktā minēto funkciju, meklēšanas mehānisms:

a) izmanto identifikatoru reģistru saskaņā ar 11. pantu;

b) izmanto pakalpojuma metadatu izdevēja (angļu *service metadata publisher – SMP*) reģistru un pakalpojuma metadatu vietrādi (angļu *service metadata locator – SML*) saskaņā ar *eDelivery* specifikācijām vai reģistra pakalpojumu ar līdzīgām iespējām, lai varētu atrast *eFTI* platformas, pamatojoties uz pieprasījumā vai papildu paziņojumā ietverto informāciju.

III NODAĻA

TEHNISKĀS SPECIFIKĀCIJAS

9. pants

Ziņojumu apmaiņa

1. Dalībvalstis nodrošina, ka to izveidotie *eFTI* vārti, kā arī to kompetento iestāžu IPP un lietotāju lietotnes sazinās un spēj saņemt paziņojumus standartizētā ziņojumu apmaiņas formātā. Saziņa starp *eFTI* vārtiem un starp *eFTI* vārtiem un *eFTI* platformām notiek, izmantojot *XML* formātu.

2. Visa saziņa starp *eFTI* vārtiem notiek kā ziņojumu apmaiņa, izmantojot *eDelivery* piekļuves punktus un *eDelivery* statiskās atklāšanas mehānismu, saskaņā ar *eDelivery* ziņojumu apmaiņas specifikācijām.

3. Ziņojumu apmaiņa, izmantojot *eDelivery* piekļuves punktus un *eDelivery* statiskās atklāšanas mehānismu, saskaņā ar *eDelivery* ziņojumu apmaiņas specifikācijām ir iespējama arī saziņā starp *eFTI* vārtiem un *eFTI* platformām.

4. Ja dalībvalsts attiecībā uz digitālajiem publiskajiem pakalpojumiem jau ir ieviesusi līdzvērtīgas, valsts līmenī noteiktas drošas ziņojumu apmaiņas specifikācijas, tā var pieņemt lēmumu nodrošināt minēto saziņu starp *eFTI* platformām un minētās dalībvalsts izveidotajiem *eFTI* vārtiem, pamatojoties arī uz šādām līdzvērtīgām ziņojumu apmaiņas specifikācijām. Šādos gadījumos dalībvalstis nodrošina, ka minētās pietiekami sīki izstrādātās un atjauninātās specifikācijas ir publiski pieejamas.

10. pants

Drošības sertifikāti

1. Dalībvalstis ar sertificētājas iestādes starpniecību izdod drošības sertifikātus *eDelivery* piekļuves punktiem, kas integrēti *eFTI* vārtos, kurus tās izveidojušas, un *eDelivery* piekļuves punktiem vai attiecīgā gadījumā līdzvērtīgam ziņojumu apmaiņas piekļuves punktam katrā *eFTI* platformā, kas saņēmusi sertifikātu no atbilstības novērtējuma struktūras, kura akreditēta to attiecīgajā dalībvalstī.

2. Dalībvalstis nodrošina, ka *eDelivery* piekļuves punkta privātās drošības atslēgas, kas integrētas *eFTI* vārtos, tiek droši glabātas un to attiecīgie digitālie sertifikāti tiek drošā veidā piegādāti starp *eFTI* vārtiem un starp *eFTI* vārtiem un *eFTI* platformām, kas savienotas ar minētajiem vārtiem.

3. Dalībvalstis nodrošina drošus mehānismus to *eFTI* platformu publisko atslēgu vai drošības sertifikātu saņemšanai, reģistrēšanai, izguvei un validēšanai, kas savienotas ar to *eFTI* vārtiem. Ja dalībvalsts saskaņā ar *eDelivery SMP* specifikācijām izveido *SMP* reģistru ar atbilstošiem drošības mehānismiem, šim nolūkam var izmantot *SMP* reģistru.

11. pants

Identifikatoru reģistrs

1. Identifikatoru reģistrs, kas minēts 8. panta 2. punkta a) apakšpunktā, ļauj uzņēmējiem, izmantojot *eFTI* platformu, augšupielādēt *eFTI* datu kopas UIS un identifikatorus, kas nodrošina minētās UIS unikālu izguvi, kā norādīts 3. punktā. Identifikatoru reģistrs ļauj augšupielādēt, aktivizēt, dezaktivizēt vai dzēst *eFTI* datu kopas un attiecīgo identifikatoru UIS.

2. UIS sastāvs ļauj izgūt *eFTI* vārtu identifikatoru, *eFTI* platformas identifikatoru un *eFTI* datu kopas unikālo identifikatoru atbilstīgi regulatīvajai informācijai, kuru uzņēmēji darījuši pieejamu attiecīgajā *eFTI* platformā, ja:

a) *eFTI* vārtu identifikatoru veido identifikators, kas ļauj to unikāli atklāt *eFTI* vidē;

b) *eFTI* platformas identifikatoru veido identifikators, kas ļauj to unikāli atklāt *eFTI* vidē;

c) *eFTI* datu kopas unikālo identifikatoru veido tāds unikāls numurs globāli unikāla identifikatora (*UUID*) formātā, ko automātiski piešķir *eFTI* platforma.

3. Reģistra atbalstīto identifikatoru sastāvs ir šāds:

a) *eFTI* datu kopas datu elementi, kas atbilst tiesiski noteiktajai informācijai, ko uzņēmēji dara pieejamu tā, kā aprakstīts Komisijas Deleģētās regulas (ES) 2024/2024 pielikuma 2. iedaļā, ar šādiem identifikācijas numuriem:

   i) eFTI39;

   ii) eFTI188;

   iii) eFTI374;

   iv) eFTI378;

   v) eFTI448;

   vi) eFTI581;

   vii) eFTI578;

   viii) eFTI618;

   ix) eFTI620;

   x) eFTI987;

   xi) eFTI1000.

b) datu elements, kas norāda, vai tiek pārvadātas bīstamas kravas, ko identificē ar šādu informāciju: datu elementa ID "eFTI1451"; norādi "Indikators, ka transportlīdzeklī atrodas bīstama krava"; tekstu "Norāde par to, vai bīstamas kravas pārvadā saskaņā ar *ADR*/*ADN*/*RID*. "Jā" nozīmē, ka transporta vienībā atrodas bīstama krava, "Nē" nozīmē, ka transportētās kravas nav iekļautas *ADR*/*ADN*/*RID* bīstamo kravu sarakstā vai ka uz bīstamajām kravām neattiecas prasības par informāciju, kā noteikts *ADR*/*ADN*/*RID* 3.5.6., 5.1.5.4.2., 5.4.1., 5.5.2.4.1. vai 5.5.3.7. punktā".

4. Identifikatoru reģistrs aktivizē UIS, lai pēc augšupielādes to darītu pieejamu vaicājumiem, un dezaktivizē to, kad ir augšupielādēts šā panta 3. punkta a) apakšpunkta ii) punktā minētais identifikators. Lai varētu izdarīt pārbaudes saskaņā ar Regulas (EK) Nr. 1072/2009 noteikumiem, katram UIS, kuram šā panta 3. punkta a) apakšpunkta vi) punktā norādītā identifikatora vērtība ir "3", kas atbilst "autotransportam", identifikatoru reģistrs dezaktivizē UIS tikai pēc Regulas (EK) Nr. 1072/2009 8. panta 2. punktā norādītā laikposma. Pēc dezaktivizēšanas reģistrs UIS un ar to saistītos identifikatorus dzēš.

IV NODAĻA

UZTURĒŠANA UN PĀRVALDĪBA

12. pants

Tehniskā atbalsta tīkls

1. Dalībvalstis izveido palīdzības dienestus šādos divos atšķirīgos līmeņos:

a) 1. līmeņa palīdzības dienests ir pieejams, lai sniegtu tehnisko atbalstu kompetento iestāžu darbiniekiem ar darbību saistītu problēmu gadījumā;

b) 2. līmeņa palīdzības dienests ir pieejams, lai sniegtu atbalstu:

i) 1. līmeņa palīdzības dienestiem, kas atbalsta kontrolierus;

ii) 1. līmeņa palīdzības dienestiem, ko izveidojuši *eFTI* platformu īpašnieki tehniskā atbalsta sniegšanai uzņēmējiem.

2. Komisija izveido 3. līmeņa palīdzības dienestu, kas:

a) sniedz tehnisko atbalstu 2. līmeņa palīdzības dienestiem tādu problēmu risināšanā, kas saistītas ar vispārējās *eFTI* apmaiņas vides darbību, arī noteikumiem, procedūrām un funkcionālās un tehniskās īstenošanas specifikācijām, kā arī ar *eFTI* kopīgo datu kopu un apakškopām, kas noteiktas īstenošanas un deleģētajos aktos, kuri ieviesti saskaņā ar Regulu (ES) 2020/1056;

b) darbojas kā atbalstītājs ar darbību saistītos jautājumos, kas skar divas vai vairākas dalībvalstis un kad ir vajadzīga koordinācija Savienības līmenī, arī jautājumos par *eFTI* vārtu tehnisko sadarbspēju un saziņu starp *eFTI* vārtiem;

c) sadarbojas ar Komisijas dienestiem, kas nodrošina īpašu programmatūru vai specifikācijas produktiem, kurus izmanto *eFTI* apmaiņas vidē, piemēram, *eDelivery*.

3. 1. līmeņa un 2. līmeņa palīdzības dienesti sazinās arī cits ar citu, lai atrisinātu jautājumus, kas skar kopīgas intereses, to attiecīgajā līmenī.

4. Palīdzības dienestu pieejamību visā Savienībā saskaņo, lai nodrošinātu minimālo kopējās pieejamības periodu darbdienās no plkst. 10.00 līdz 16.00 pēc Viduseiropas laika (*CET*/*CEST*), izņemot valsts svētku dienas. Nedēļas nogalēs un valsts svētku dienās tiek nodrošināts ārkārtējs pakalpojums, kur pieejams vismaz viens dežūrdarbinieks, kas sniedz atbalstu steidzamos jautājumos, kuri nopietni ietekmē *eFTI* apmaiņas vides darbību valsts vai Savienības līmenī.

5. Visi palīdzības dienesti izmanto īpašus palīdzības rīkus, kas ļauj unikāli identificēt katru tehniskā atbalsta pieprasījumu un veikt turpmākus ar to saistītus pasākumus, arī tad, ja pieprasījuma risināšanai vajadzīga saziņa starp palīdzības dienestiem.

6. Palīdzības dienesti glabā reģistrus, kuros iekļauti visi palīdzības pieprasījumi un to vēsture, un regulāri apkopo ziņojumus par savu darbību.

7. Dalībvalstis cita citai un Komisijai paziņo savu 2. līmeņa palīdzības dienestu kontaktinformāciju.

8. Palīdzības dienestu pieejamības sākuma datums ir Regulas (ES) 2020/1056 5. panta 1. punktā minētais datums. Palīdzības dienestu kopējās pieejamības minimālā laikposma atbilstību novērtē 12 mēnešu laikā pēc minētā datuma.

13. pants

Operatīvā atbalsta tīkls

1. Izveido īpašu darba grupu – apakšgrupu saskaņā ar Lēmumu C(2018) 5921 izveidotajai ekspertu grupai –, kurai ir pilnvaras nodrošināt, ka *eFTI* darbības notiek vajadzīgajā kvalitātes līmenī.

2. Dalībvalstu ieceltie darba grupas locekļi darbojas arī kā "*eFTI* valstu kontaktpunkti".

3. Darba grupas locekļi sadarbojas un regulāri tiekas, lai cita starpā:

a) sniegtu jaunāko informāciju par *eFTI* apmaiņas vides darbības statusu;

b) palīdzētu Komisijas dienestiem to centienos atrisināt tehniskās un darbības problēmas, par kurām ziņojušas dalībvalstis vai 3. līmeņa palīdzības dienests un kurām vajadzīga koordinācija un darbības norādījumi Savienības līmenī;

c) palīdzētu Komisijai izstrādāt tehnisko norādījumu dokumentu, lai sekmētu šīs regulas īstenošanu.

V NODAĻA

NOBEIGUMA NOTEIKUMI

14. pants

Stāšanās spēkā un piemērošana

Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

To piemēro no šīs regulas spēkā stāšanās dienas.

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

Briselē, 2024. gada 5. jūlijā

Komisijas vārdā –
priekšsēdētāja
Ursula VON DER LEYEN